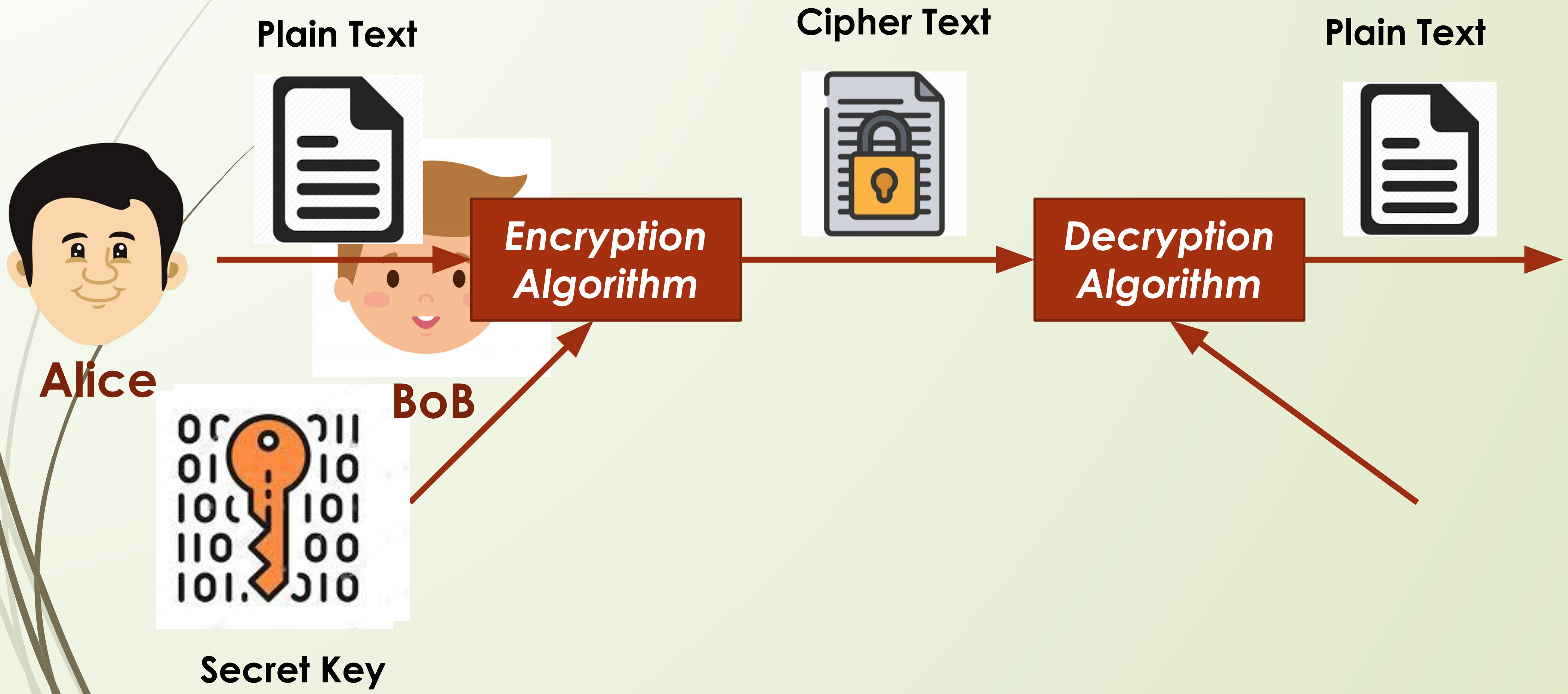
Symmetric Key Encipherment

Outline

- Cryptosystem
- Modular Arithmetic
- Additive Cipher
- Ceaser Cipher
- Multiplicative Cipher
- Affine Cipher
- Monoalphabetic Substitution Cipher
- Playfair
- Vigenere
- Autokey
- Hill Cipher
- Transposition Ciphers
- Block cipher vs Stream Ciphers

Basic Cryptosystem



Continue…

- **Plain Text –** Original Message
- **Cipher Text -** the scrambled message produced as output
- **Encryption Algorithm -** performs various substitutions and transformations on the plaintext
- **Decryption Algorithm -** the encryption algorithm run in reverse
- **Secret Key -** input to the encryption algorithm
- **The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.**

Types of Cryptographic

- Cryptographic systems are characterized along three independent dimensions:

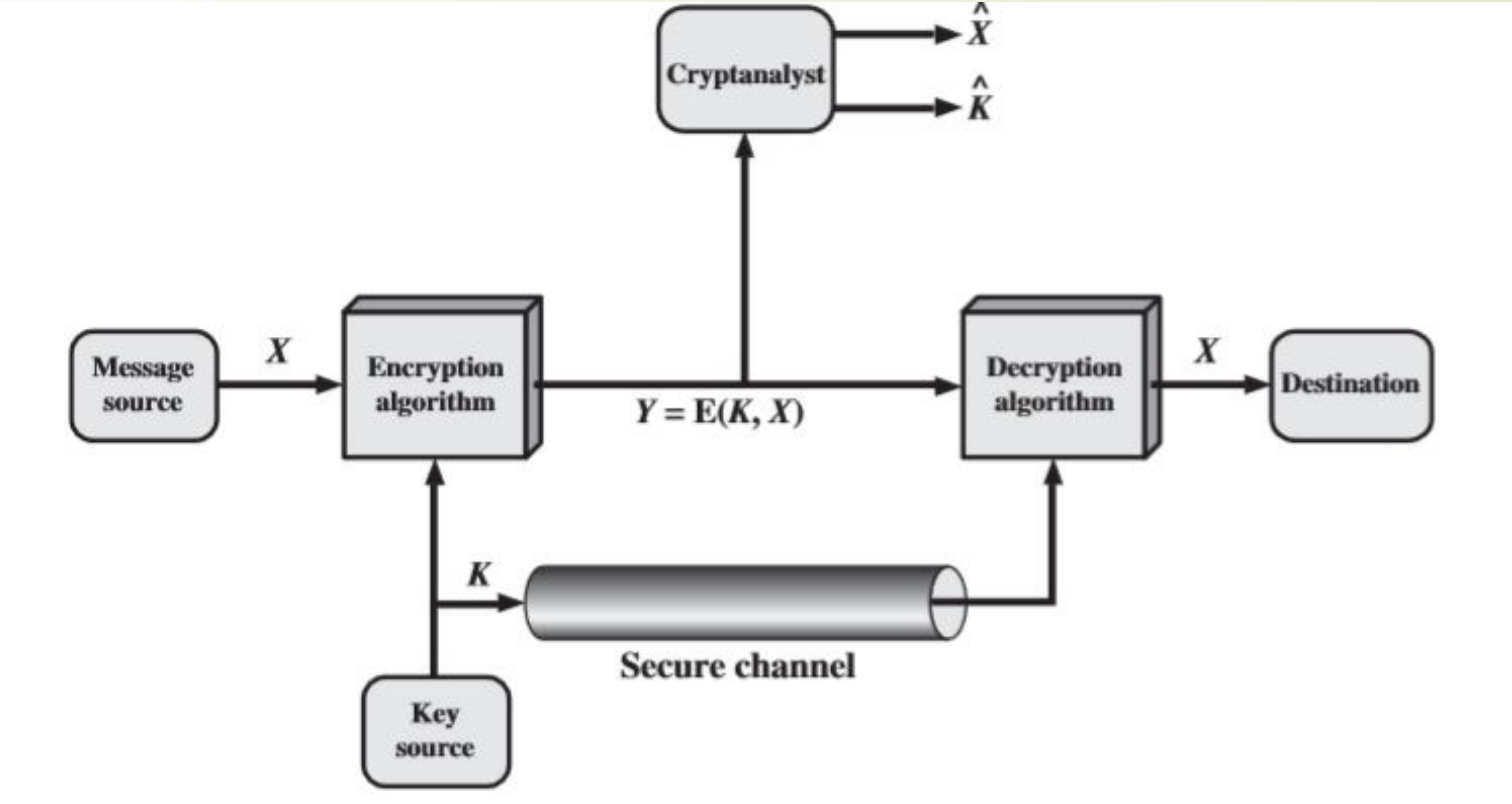
1. **The type of operations** used for transforming plaintext to ciphertext.

- All encryption algorithms are based on two general principles: **substitution**, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, **and transposition,** in which elements in the plaintext are rearranged.
- The fundamental requirement is that no information be lost (that is, that all operations are reversible).

Continue...

2. ***The number of keys used.*** If both sender and receiver use **the same key**, the system is referred to **as symmetric, single-key, secret-key, or conventional encryption**. If the sender and receiver **use different keys**, the system is referred to as **asymmetric, two-key,or public-key** encryption.
3. **The way in which the plaintext is processed**.

A **block cipher** processes the input one block of elements at a time, producing an output block for each input block. A **stream cipher** processes the input elements continuously, producing output one element at a time, as it goes along.



Model of Symmetric Cryptosystem

Process of Cryptosystem

- In its most basic form, two people, often denoted as Alice and Bob, have agreed on a particular **secret key**.
- At some later time, Alice may wish to send a secret message to Bob (or Bob might want to send a message to Alice).
- **The key** is used to **transform** the **original message** (which is usually termed the **plaintext**) into **a scrambled** form that **is unintelligible** to anyone who does not possess the key.
- **This process** is called **encryption** and the **scrambled message** is called the **ciphertext.**
- When **Bob receives the ciphertext**, he can use **the key** to **transform the ciphertext back into the original plaintext**; this is the **decryption process**.

Continue..

- A **cryptosystem** constitutes a complete specification of the keys and how they are used to encrypt and decrypt information.
- The **techniques** used by the adversary **to attempt to "break" the cryptosystem** are termed **cryptanalysis.**
- The **most obvious type of cryptanalysis** is to try to **guess the key**.
- An attack wherein the adversary tries to decrypt the ciphertext with every possible key in turn is termed an **exhaustive key search**.

Continue...

- When the **adversary tries the correct key**, the **plaintext** will be found, but when **any other key** is used, the “decrypted” ciphertext will likely **be random Messages**.
- So an obvious first step in **designing a secure cryptosystem** is to specify **a very large number of possible keys**, so many that **the adversary will not be able to test them all** in **any reasonable amount of time**.

Continue .....

If , Plaintext = P Ciphertext = C Key = K

Encryption : $C = E_k (P)$

Decryption : $P = D_K (C)$

Secret Key Cryptography/ Symmetric Key Cryptosystem

- The model of cryptography described above is usually called **secret-key cryptography**. This indicates that there is **one secret key**, which is known to both Alice and Bob.
- That is, the key is a “secret” that Is known to two parties.
- This key is employed both to encrypt plaintexts and to decrypt ciphertexts.
- The **actual encryption and decryption functions** are thus **inverses of each** other.

Drawbacks of Secret Key Cryptosystem

- **Alice and Bob** must somehow be able to **agree on the secret key ahead of time** (before they want to send any messages to each other).
- This might be straightforward if Alice and Bob are in the same place when they choose their secret key.

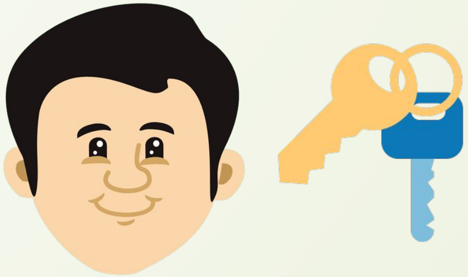
But what if Alice and Bob are far apart, say on different continents???

Public key Cryptography/ Asymmetric Cryptography

- Two keys instead of one.
- One is Public key and one is private key.
- **One key** would be used **to encrypt** the message.
- **Another key** would be used ***to decrypt*** the message.

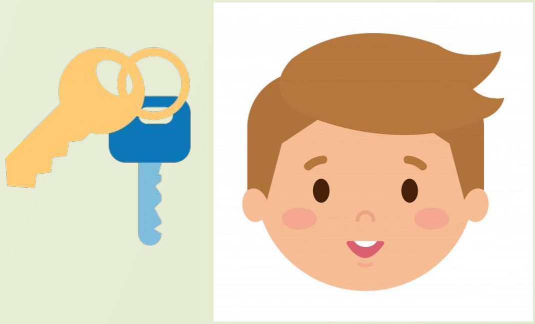
Public Key Cryptosystem

Private Key- Alice
Public Key- Alice

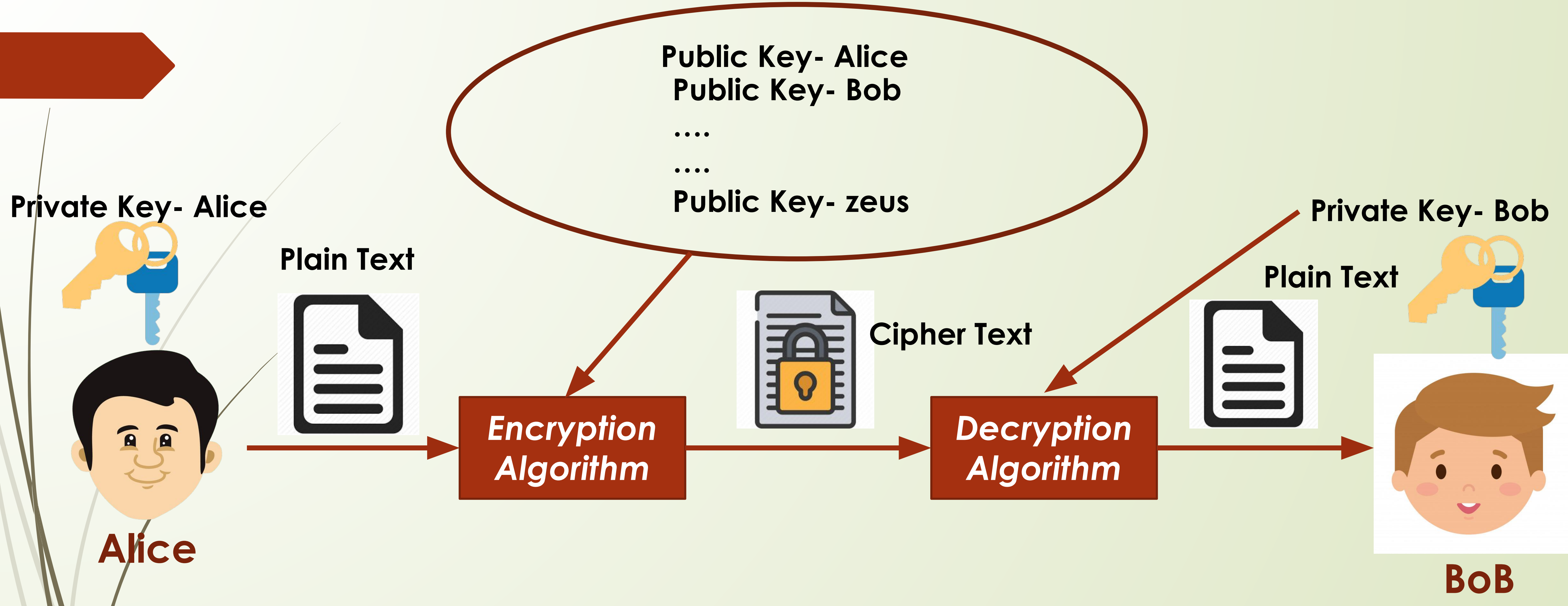


Alice

Private Key- Bob
Public Key- Bob



BoB



Public Key Cryptosystem

Cryptosystem

Definition 2.1: A ***cryptosystem*** is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

1. $\mathcal{P}$ is a finite set of possible ***plaintexts***;
2. $\mathcal{C}$ is a finite set of possible ***ciphertexts***;
3. $\mathcal{K}$, the ***keyspace***, is a finite set of possible ***keys***;
4. For each $K \in \mathcal{K}$, there is an ***encryption rule*** $e_K \in \mathcal{E}$ and a corresponding ***decryption rule*** $d_K \in \mathcal{D}$. Each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ are functions such that $d_K(e_K(x)) = x$ for every plaintext element $x \in \mathcal{P}$.

Continue…

- A practical cryptosystem should satisfy
  - Each **encryption function ek** and **each decryption function dk** should be efficiently computable.
  - An opponent, upon seeing the **ciphertext string y**, should be unable to determine the key k that was used, or the plaintext string x.

Kerckhoff’s Principle

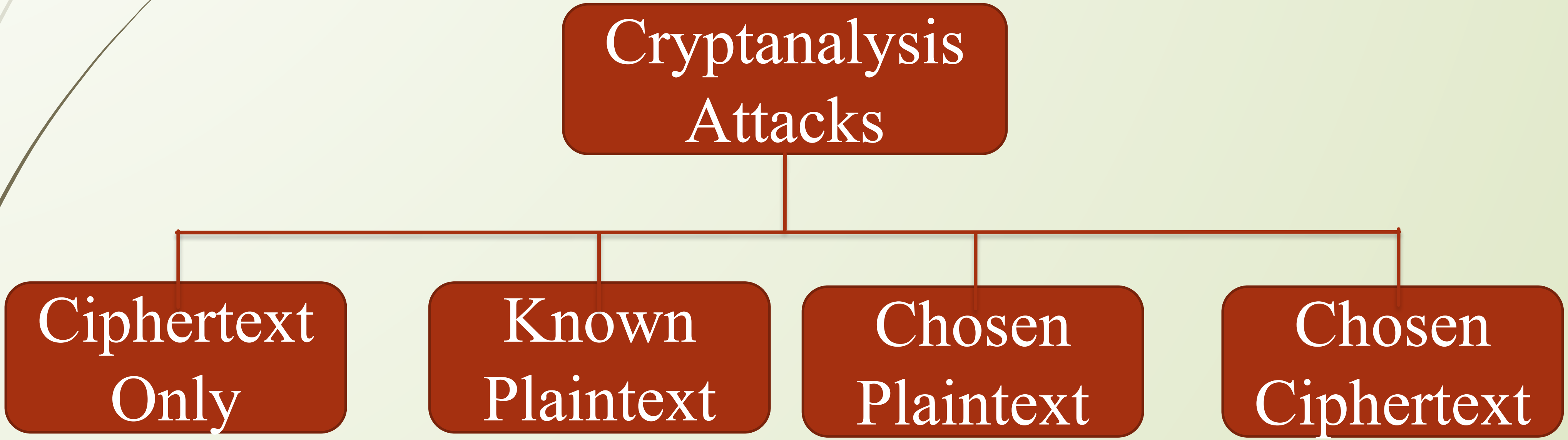
- For more security – encryption/decryption algorithm + key should be hidden
- Based on kerckhoff’s principle, one should always assume that the adversary knows encryption/decryption algorithm
- Resistance of cipher to attack must be based only on secrecy of the key
- Key domain for each algorithm should be so large that it makes it difficult for the adversary to find the key

Cryptanalysis Attack

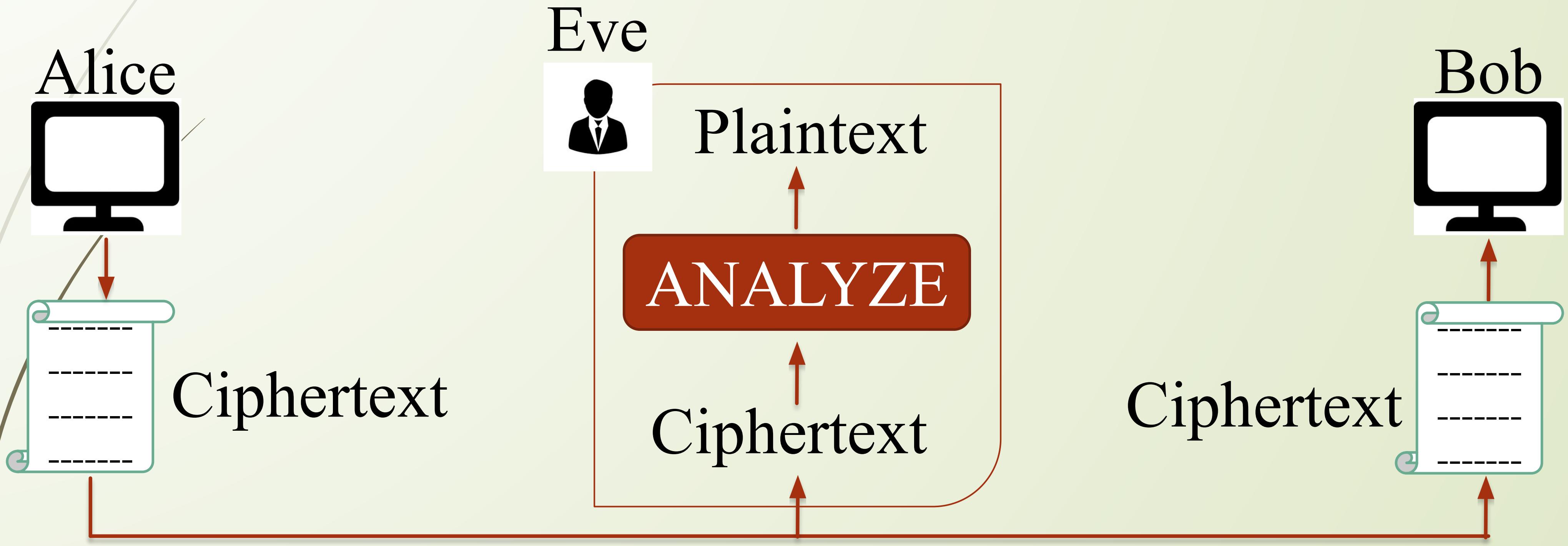
- Cipher-text Only attack
- Known Plaintext
- Chosen Ciphertext
- Chosen- plaintext

Cryptanalysis Attacks

- As cryptography is science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes



CipherText – only attack



Brute-Force Attack : Exhaustive – key search method

- We assume that Eve knows the algorithm and knows the key domain
- Using intercepted cipher, Eve decrypts the ciphertext with every possible key until the plaintext makes sense
- To prevent this type of attack, the number of keys must be very large

Statistical Attack :

- Cryptanalyst can benefit from some inherent characteristics of the plaintext language to launch a statistical attack
- Cryptanalyst find most frequently used character in ciphertext
- Based on that assume the key and use it to decrypt the message
- To prevent this attack, cipher should hide the characteristics of the language

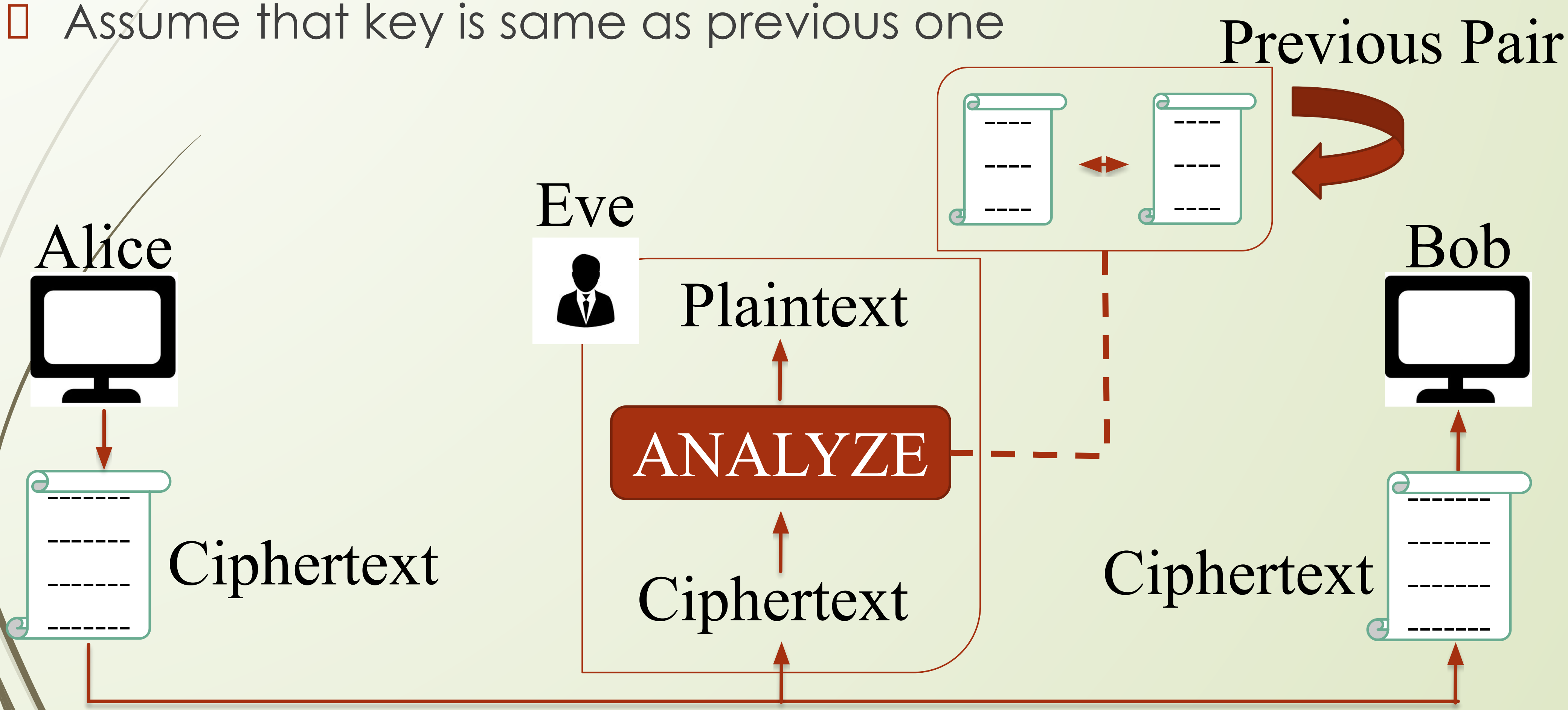
Pattern Attack :

- Some ciphers may hide characteristics of the language but may create some pattern in the ciphertext

- It is important to use ciphers that make the ciphertext look as random as possible

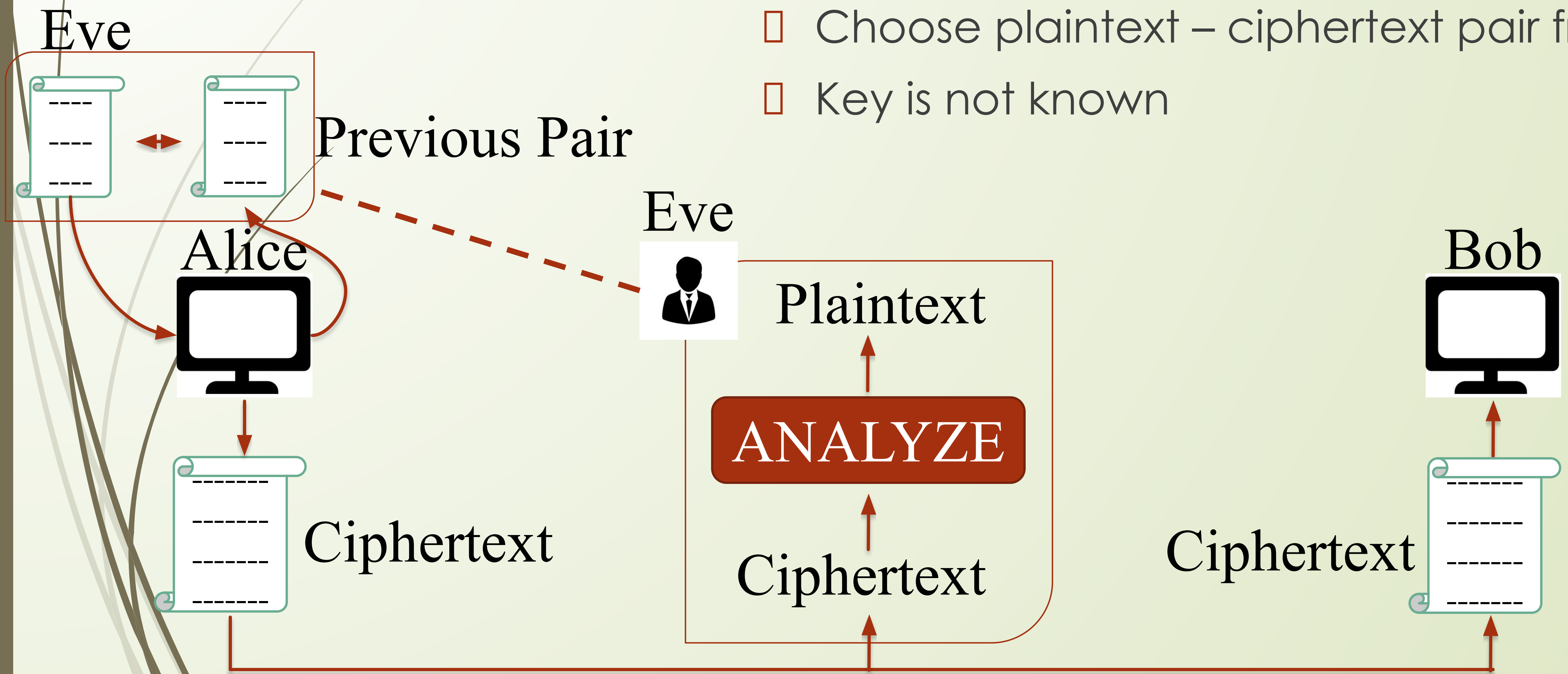
Known - plaintext attack

- Access to some plaintext/ciphertext pair
- Assume that key is same as previous one



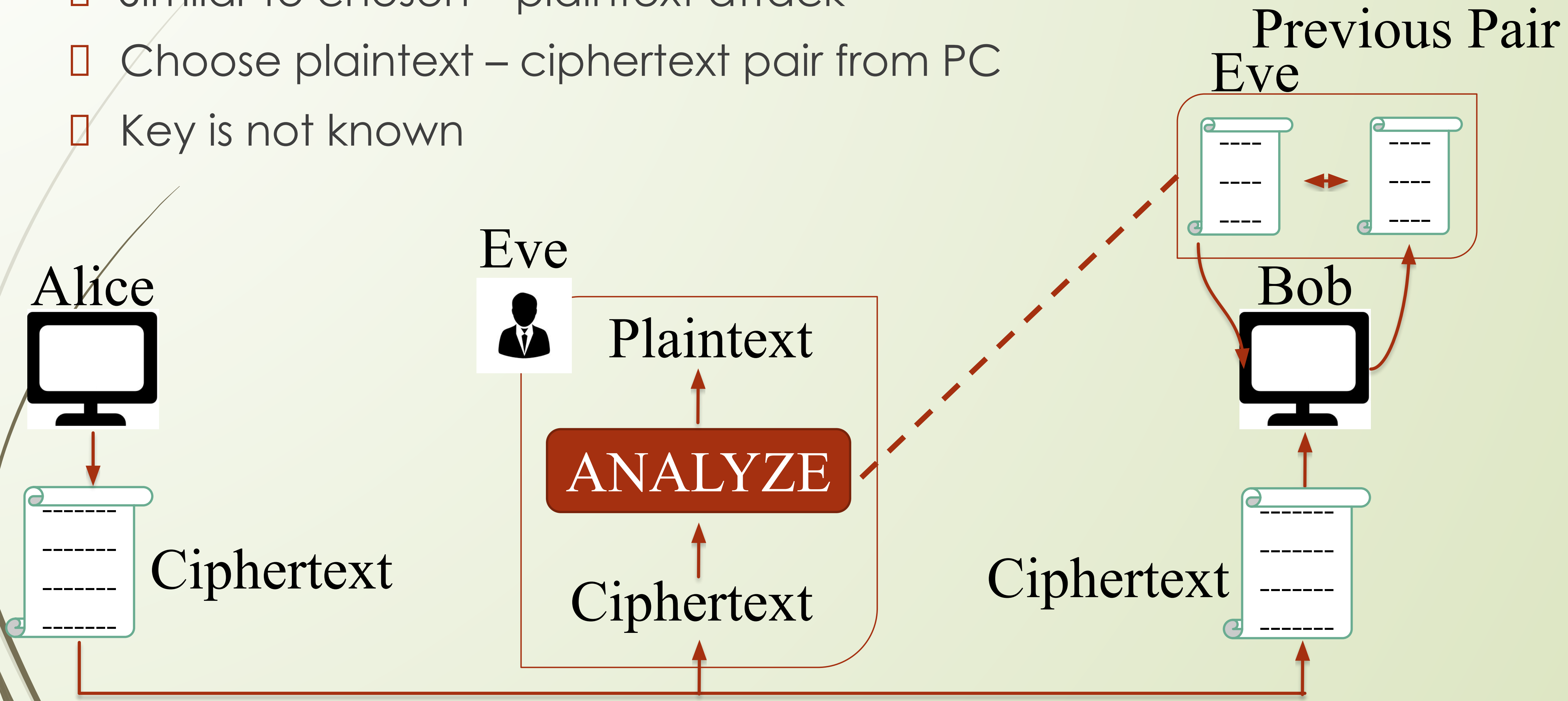
chosen - plaintext attack

- Similar to known – plaintext attack
- Choose plaintext – ciphertext pair from PC
- Key is not known



chosen - ciphertext attack

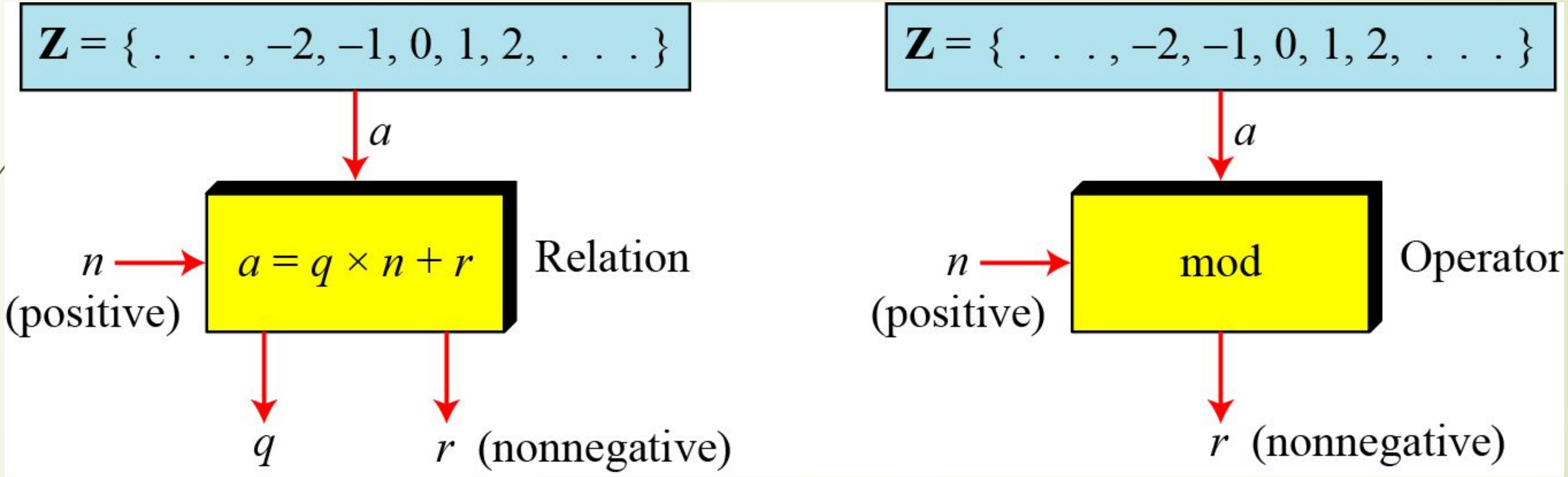
- Similar to chosen – plaintext attack
- Choose plaintext – ciphertext pair from PC
- Key is not known



MODULAR ARITHMETIC

- **The division relationship** ($a = q \times n + r$) has **two inputs (a and n)** and **two outputs (q and r).**
- In **modular arithmetic**, we are interested in only one of the outputs, **the remainder r**.
- **The modulo operator** is shown as **mod**.
- The **second input (n)** is called the **modulus**.
- **The output r** is called **the residue**.

Division algorithm and modulo operator



Examples:

- Find the result of the following operations:

a. $27 \bmod 5$

b. $36 \bmod 12$

c. $-18 \bmod 14$

d. $-7 \bmod 10$

Solution

a. Dividing 27 by 5 results in $r = 2$
b. Dividing 36 by 12 results in $r = 0$.
c. Dividing -18 by 14 results in $r = -4$. After adding the modulus $r = 10$
d. Dividing -7 by 10 results in $r = -7$. After adding the modulus to -7, $r = 3$.

Zn- The set of least residues modulo n

- The modulo operation creates a set, which in modular arithmetic is referred to as **the set of least residues modulo n, or Zn.**

Some Z_n sets

$$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

$$\mathbf{Z}_2 = \{ 0, 1 \} \qquad \mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \} \qquad \mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$$

Monoalphabetic Ciphers

- A **character in plaintext** is always **changed to the same character**(or symbol) in cipher text **regardless of its position in the text**.
- **Relationship** between **a symbol in plaintext** to **a symbol in ciphertext** is always **one-to-one**.

Shift Cipher
Additive Cipher
Ceaser Cipher

Shift Cipher

- Simplest monoalphabetic cipher.
- To perform mathematical operations on plain text and ciphertext, we need to assign numerical values to each letter.

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext and ciphertext in Z_{26}

Shift Cipher

Cryptosystem 2.1: *Shift Cipher*

Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. For $0 \leq K \leq 25$, define

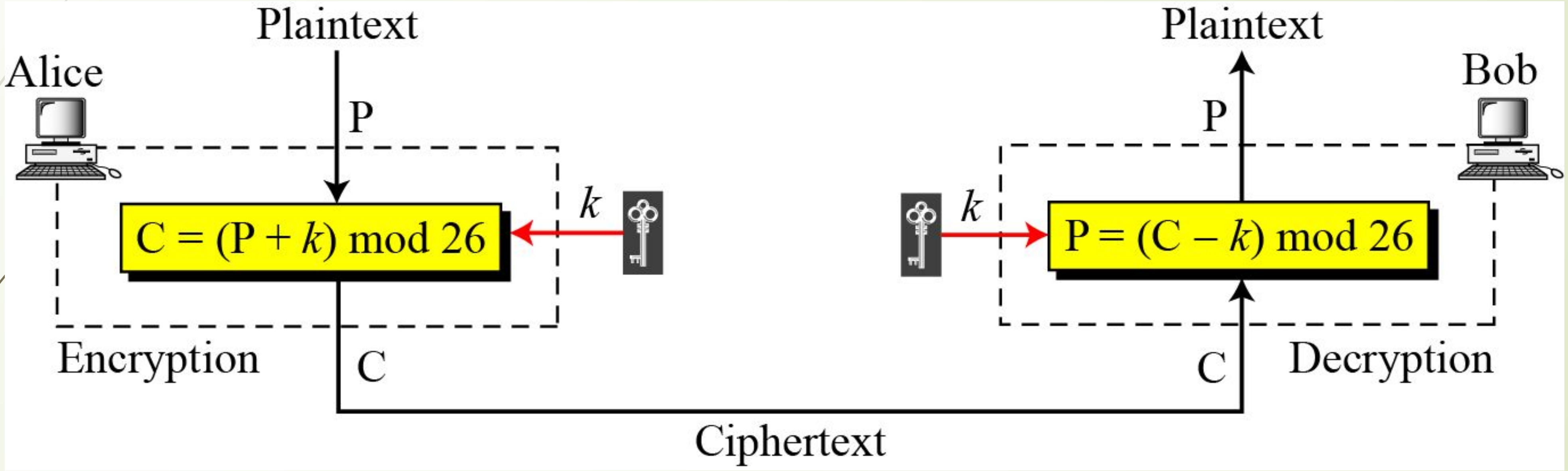
$$e_K(x) = (x + K) \bmod 26$$

and

$$d_K(y) = (y - K) \bmod 26$$

$(x, y \in \mathbb{Z}_{26})$.

Continue...


Plaintext
Alice
P
k
C = (P + k) mod 26
Encryption
C
Ciphertext
Plaintext
Bob
P
k
P = (C – k) mod 26
C
Decryption

Continue...

- Also known as **additive cipher** on the basis of their **mathematical nature**.
- Also known as **ceasar cipher as Julius Ceasar** used an additive cipher for communication **with key=3**.
- Shift Cipher means “Shift key characters down/up”
- **In Additive Cipher, plaintext, ciphertext and key are integers in Z_{26}.**

Example:

Encryption

1. Plaintext =“hello” key=15
2. Plaintext=“this is an exercise” key=20

Example

Decryption

1. Ciphertext="wtaad" key=15
2. Ciphertext="UVACLYFZLJBYL" . Find the key.

Cryptanalysis- Bruteforce attack

Ciphertext: UVACLYFZLJBYL

K = 1 → **Plaintext:** tuzbkxeykiaxk
K = 2 → **Plaintext:** styajwdxjhzwj
K = 3 → **Plaintext:** rsxzivcwigyvi
K = 4 → **Plaintext:** qrwyhubvhfxuh
K = 5 → **Plaintext:** pqvxgtaugewtg
K = 6 → **Plaintext:** opuwfsztfdvsf
K = 7 → **Plaintext:** notverysecure

Statistical Analysis

Letter	Frequency	Letter	Frequency	Letter	Frequency	Letter	Frequency
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Frequency of characters in English

Continue...

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

Frequency of diagrams and trigrams

statistical attack

- **Example: Cipher text is like below:**

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

Solution

- When Eve tabulates the frequency of letters in this ciphertext,
- gets: I =14, V =13, S =12, and so on.
- The most common character is I with 14 occurrences.
- That means, E might be replace by I.
- So E=(I-key) mod 26.
- So key can be 4.

Continue…

- If we take key=4,
- Plain text will be

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Monoalphabetic Substitution Cipher

Monoalphabetic Substitution Cipher

- Because **additive cipher** have **small key domains**, they are very vulnerable to brute-force attack.
- **A better solution** is **to create a mapping between each plaintext character and the corresponding ciphertext character**.
- Alice and Bob can agree on a table showing the mapping for each character.

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

Example:

- **Plain Text : welcome to charusat**

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

- **CipherText: PRDAYQRIYACNHJVNI**

Continue…

Cryptosystem 2.2: *Substitution Cipher*

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. $\mathcal{K}$ consists of all possible permutations of the 26 symbols $0, 1, \ldots, 25$. For each permutation $\pi \in \mathcal{K}$, define

$$e_{\pi}(x) = \pi(x),$$

and define

$$d_{\pi}(y) = \pi^{-1}(y),$$

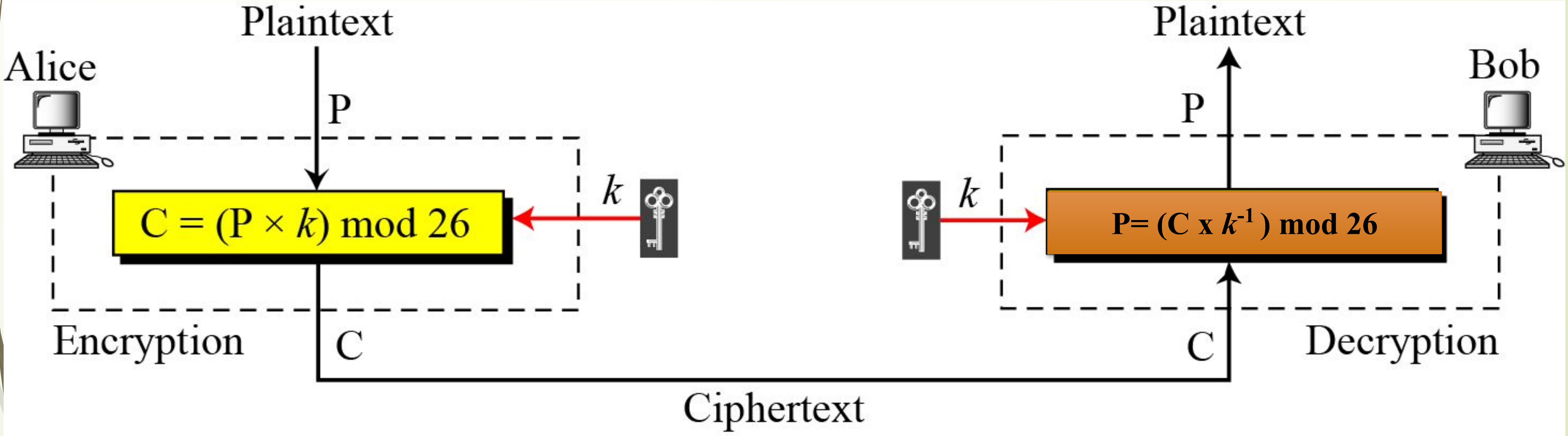
where π^{-1} is the inverse permutation to π.

Cryptanalysis

- No of Possible keys: 26!
- So it is computationally infeasible for computer to find out the correct key in finite time.
- **Statistical attack or Frequency Analysis attack**

Multiplicative cipher

Multiplicative cipher



Continue…

- In a multiplicative cipher, the plaintext and ciphertext are integers in **Z_{26}**.
- the key is an integer **in Z_{26}*.**
- **Z_{26}* :** subset of Zn which includes **integers** in Zn that **have unique multiplicative inverse.**
- **If GCD of (a,n) =1 then multiplicative inverse of a in Zn exists.**

Example

- Use Multiplicative cipher to encrypt the message “hello” with a key =7.
- **Answer:**

Plaintext= hello

P1=h	**c1= (P1 * K) mod 26**	**c1=(7*7)mod 26= 23 ->x**
P2=e	**c2= (P2 * K) mod 26**	**c2=(4*7)mod 26= 2 ->c**
P3=l	**c3= (P3 * K) mod 26**	**c3=(11*7)mod 26=25 ->z**
P4=l	**c4= (P4 * K) mod 26**	**c4=(11*7)mod 26=25 ->z**
P5=0	**c5= (P5 * K) mod 26**	**c5=(14*7)mod 26=20->u**

Multiplicative Inverse

- In Zn two numbers a and b are the multiplicative inverse of each other if

a X b ≡ 1 (mod n)

(a* b is congruence to 1 mod n)

Meaning: **(a *b) mod n= 1 mod n**.

For more detail

Continue…

- If a * b mod n =1 , a and b are multiplicative inverse of each other in Zn.
- Example:
- **Z_{10} = {0,1,2,3,4,5,6,7,8,9} find multiplicative inverse of 3.**

- **3 * m mod 10=1**
- **m will be 7 as (7*3) mod 10 will be 1.**

Find Multiplicative inverse

- 23 in Z_{100}
- 12 in Z_{26}
- 15 in Z_{26}
- 7 in Z_{26}

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
	100	23		0	1	

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23		0	1	

Q= R1 / R2

Q= 100/ 23 = 4

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	

R = R1 % R2

R= 100% 23 = 8

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4

T =T1 - Q * T2

T = 0 – 4 * 1= -4

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
	23	8		1	-4	

Solution

Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
2	23	8		1	-4	

Q= R1 / R2

Q= 23/8 = 2

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	

R= R1 % R2

R= 23 % 8 = 7

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9

T = T1 - Q * T2

T = 1 – (2 * -4)= 9

Solution

Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
	8	7		-4	9	

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13

Q= R1 / R2

Q= 8/7 = 1

R= R1 % R2

R= 8 % 7 = 1

T = T1 - Q * T2

T = -4 – (1 * 9)= -13

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
	7	1		9	-13	

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100

Q= R1 / R2

Q= 8/7 = 1

R= R1 % R2

R= 8 % 7 = 1

T = T1 - Q * T2

T = 9 – (7 * -13)= 100

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0		-13	100	

Solution
Multiplicative inverse of 23 in Z_{100}

Q	R1	R2	R	T1	T2	t
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0		-13	100	

As r1=1 stop propagating further take t1 from the table.
So -13 mod 100=87 will be the multiplicative inverse of 23 in Z_{100}

Continue…

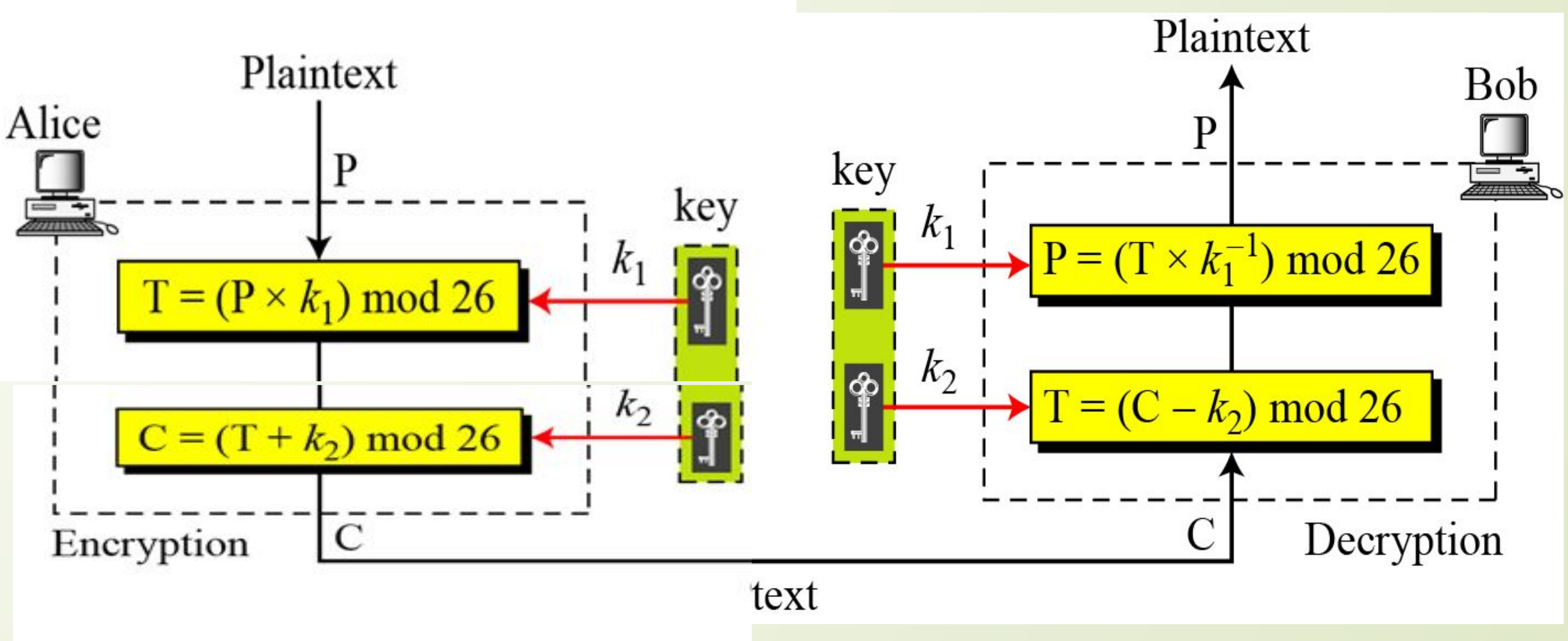
- **Multiplicative Inverse of 23 in Z100 is 87.**

Example

- Find the key domain of Z_{26}*?
- Find the Ciphertext for message =“This is exercise” with key=15.
- Find the plain text for ciphertext=XCZZU for key=7.

Affine cipher

Affine Cipher



$$C = (P \times k_1 + k_2) \bmod 26 \qquad\qquad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

Use an affine cipher to encrypt the message “hello” with the key pair (7, 2).

P: h $\rightarrow$ 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 $\rightarrow$ Z
P: e $\rightarrow$ 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 $\rightarrow$ E
P: l $\rightarrow$ 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 $\rightarrow$ B
P: l $\rightarrow$ 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 $\rightarrow$ B
P: o $\rightarrow$ 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 $\rightarrow$ W

Use an affine cipher to decrypt the message "PWUFFOGWCHFDWIWEJOUUNJORSMDWRHVCMWJUPVCCG" with the key pair (11, 4).

Solution:

"best time of the year is spring when flowers bloom"

No of Possible keys

Here K1 will be from Z_{26}* and k2 will be from Z_{26}.

- Here No of **elements** in **Z_{26}=26**
- No of **elements** in **Z_{26}*=12**.

- So **no of possible** combinations will be = **12 * 26=312**.
- If we **Ignore** the key pair **(1,0)**, as it doesn't make change in plaintext at all. No of possible keys in that case will be **311**.

The additive cipher is a special case of an affine cipher in which
$k_1 = 1$.

The multiplicative cipher is a special case of affine cipher in which $k_2 = 0$.

What are the possible no of keys for Z_{60}??

- No of elements in Z_{60}= 60.
- No of elements in Z_{60}^*= 16.

- So total no of possible keys= 60 *16=960.

Euler's Phi- Function

- Euler's Phi-function Ø(n) finds the no of integers that are both smaller than n and relatively prime to n.
- **Z_n* = no of elements smaller from n and relatively prime to n.**

No of elements in Zn*= Ø(n)

- **Relatively Prime: Two positive integer , a and b, are relatively prime if GCD(a,b) = 1.**
- **GCD the largest positive integer number that divides both the numbers without leaving any remainder.**
- **1 is relatively prime with any integer.**

Rules for finding value of **Ø(n)**

1. Ø(1)=0.
2. Ø(p)=p-1 if p is prime.
3. Ø(m X n)= Ø(m) * Ø(n) if m and n are relatively prime.
4. Ø(p^e)= $p^e - p^{e-1}$

Find the GCD of given nos.

- 23,67
- 12,15
- 14,18
- 16,81
- 15,16
- 6,35

Exercise

Rules

1. Ø(1)=0.
2. Ø(p)=p-1 if p is prime.
3. Ø(m X n)= Ø(m) * Ø(n) if m and n are relatively prime.
4. $Ø(p^e)= p^e – p^{e-1}$

Find the value of below:

1. Ø(13)
2. Ø(10)
3. Ø(30)
4. Ø(240)
5. Ø(60)
6. Ø(19)

Solution

1. Ø(13) =13-1=12 (As 13 is prime, According to Rule 2, Ø(13))
2. Ø(10) = Ø(5 X 2) (According to Rule no 3)
   = Ø(5) * Ø(2) (According to Rule no 3, 5 and 2 are relatively prime)
   = 5-1 * 2-1 (According to Rule no 2, 5 and 2 are prime numbers)
   = 4 * 1 = 4
3. Ø(240) = Ø(120 * 2)
   = Ø(60 * 2 * 2)
   = Ø(30 * 2 * 2 *2)
   = Ø(15 * 2 * 2 * 2 * 2)
   = Ø(5 * 3 * 2^4)
   = Ø(5) * Ø(3) * Ø(2^4) = 4 * 2 * (2^4 – 2^3) =8 * 8 =64

Rule no 4

Continue…

1. $\varnothing(30) = \varnothing(5 * 3 * 2)$ (According to **Rule no 3**, 5, 3 and 2 are relatively prime)

   $= \varnothing(5) * \varnothing(3) * \varnothing(2)$

   $= 4 * 2 * 1$ (According to **Rule no 2**, 5, 3 and 2 are prime numbers)

   $= \mathbf{8}$

Find the No of possible keys for Z_{30}.

- No of elements in Z_{30}= 30.
- What will be no of elements in Z_{30}*=??
- **Solution**
- **Ø(30) = Ø(15 * 2) =Ø(15) * Ø(2) = Ø(5 * 3) * Ø(2)**

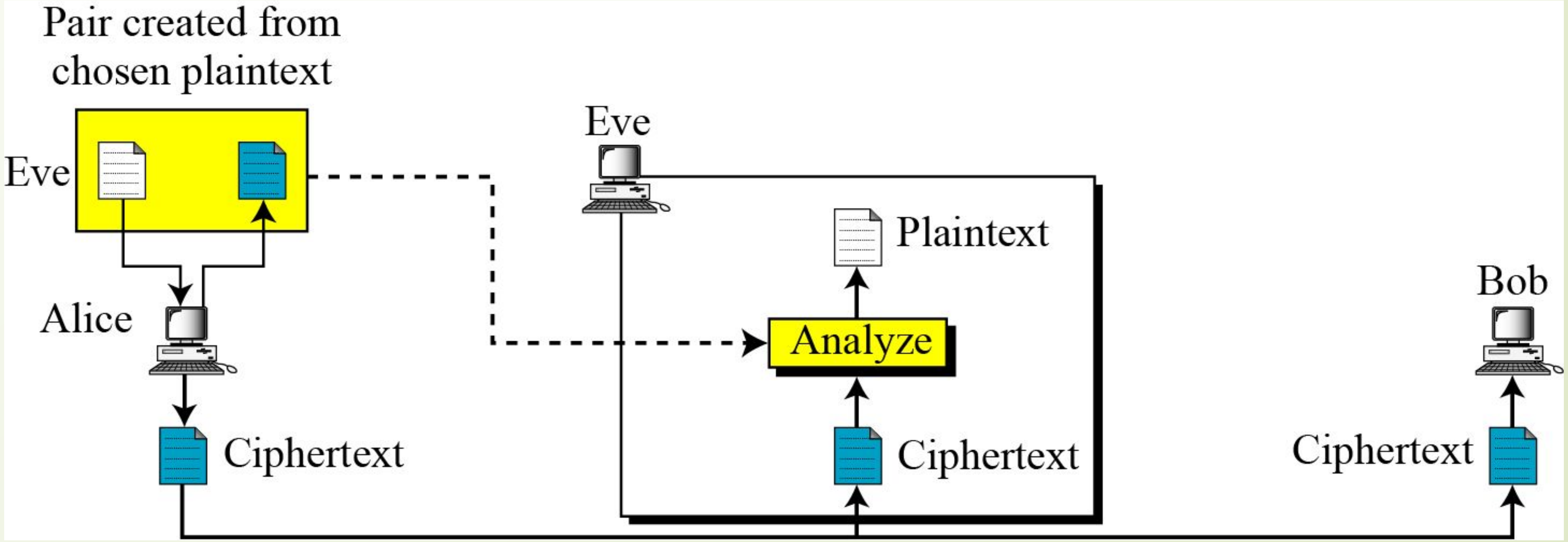
  = Ø(5) * Ø(3) * Ø(2)

  = 4 * 2 * 1

  =8

So no of possible keys= 30 * 8 =240

Chosen-Plaintext Attack



Cipher message is
“PWUFFOGWCHFDWIWEJOUUNJORSMDWR
HVCMWJUPVCCG”
perform chosen plain text attack.

Example:
For algorithm 1
Plainttext:et ciphertext:WC
For algorithm 2
Plainttext:et Ciphertext:WF

We can also solve a set of linear equations with the same modulus if the matrix formed from the coefficients of the variables is invertible.

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &\equiv b_1\\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &\equiv b_2\\
&\vdots\\
a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &\equiv b_n
\end{aligned}$$

a. Equations

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \vdots & \vdots & & \vdots\\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1\\ x_2\\ \vdots\\ x_n \end{bmatrix} \equiv \begin{bmatrix} b_1\\ b_2\\ \vdots\\ b_n \end{bmatrix}$$

b. Interpretation

$$\begin{bmatrix} x_1\\ x_2\\ \vdots\\ x_n \end{bmatrix} \equiv \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \vdots & \vdots & & \vdots\\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}^{-1} \begin{bmatrix} b_1\\ b_2\\ \vdots\\ b_n \end{bmatrix}$$

c. Solution

Polyalphabetic Cipher

Polyalphabetic Cipher

- In polyalphabetic substitution, each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.

Autokey cipher

Autokey Cipher

- Simple polyalphabetic Cipher
- Key is the stream of subkeys, in which each subkey is used to encrypt the corresponding character in the plaintext.
- The key K= K1 K2 K3….Kn
- The K1 will be predetermined value shared secretly between communicating parties.
- The K2 will be the first plaintext character.
- The K3 will be the second plaintext character and so on…

Autokey Cipher

$P = P_1P_2P_3 \ldots$ $\qquad C = C_1C_2C_3\ldots$ $\qquad k = (k_1, P_1, P_2, \ldots)$

Encryption: $C_i = (P_i + k_i) \bmod 26$ $\qquad$ Decryption: $P_i = (C_i - k_i) \bmod 26$

Example

- Assume that Alice and Bob agreed to use an autokey cipher with initial key value k1 = 12. Now Alice wants to send Bob the message "Attack is today". Enciphering is done character by character.

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P's Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	*12*	*00*	*19*	*19*	*00*	*02*	*10*	*08*	*18*	*19*	*14*	*03*	*00*
C's Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	**M**	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**

Example

- Plaintext= “the house is being sold tonight”
- Key=7

P.T.	T	H	E	H	O	U	S	E	I	S	B	E	I	N	G	S	O	I	D	T	O	N	I	G	H	T
P.T	19	7	4	7	14	20	18	4	8	18	1	4	8	13	6	18	14	8	3	19	14	13	8	6	7	19
Key	7	19	7	4	7	14	20	18	4	8	18	1	4	8	13	6	18	14	8	3	19	14	13	8	6	7
C.T	26	26	11	11	21	34	38	22	12	26	19	5	12	21	19	24	32	22	11	22	33	27	21	14	13	26
						8	12										6				7	1				
C.T	**A**	**A**	**L**	**L**	**V**	**I**	**M**	**W**	**M**	**A**	**T**	**F**	**M**	**V**	**T**	**Y**	**G**	**W**	**L**	**W**	**H**	**B**	**V**	**O**	**N**	**A**

Cryptanalysis of Autokey

- Hides the single letter frequency statistics of the plaintext.
- Vulnerable to brute force attack as the first subkey can be only one of the 25 characters.

Vigenere cipher

Vigenere Cipher

- It uses different strategy to create the key stream.
- The key stream is repetition of an initial secret key stream of length m.

$$P = P_1P_2P_3 \ldots \qquad C = C_1C_2C_3 \ldots \qquad K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$$

$$\text{Encryption: } C_i = P_i + k_i \qquad \text{Decryption: } P_i = C_i - k_i$$

We can encrypt the message “She is listening” using the 6-character keyword “PASCAL”.

Example:

- Plain text: “She is listening”
- Key: “PASCAL”

P.T.	S	H	E	I	S	L	I	S	T	E	N	I	N	G
P.T	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Key	P	A	S	C	A	L	P	A	S	C	A	L	P	A
Key	15	0	18	2	0	11	15	0	18	2	0	11	15	0
C.T	7	7	22	10	18	22	23	18	11	6	13	19	2	6
C.T	H	H	W	K	S	W	X	S	L	G	N	T	C	G

Vigenere Cipher- Continue..

- The Vigenere cipher can be considered as a combination of m additive cipher.

Playfair cipher

Play Fair Cipher

- **Before Encryption Rules:**
  - If two letters in a pair are the same
    - add bogus letter
  - If no of characters in plaintext is odd
    - add bogus letter at the end
- **For Encryption Rules:**
  - If 2 letters in a pair are located in the same row of the secret key, corresponding encrypted character for each letter is next letter to the right in the same row
  - If 2 letters in a pair are located in the same column of secret key, corresponding encrypted character for each letter is beneath it in same column
  - If 2 letters in a pair are not in the same row or column of the secret key, the corresponding encrypted character for each letter is a letter that is in its own row but in same column as the other letter

Continue..

- Key size : 25!

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Hill cipher

Hill Cipher

Plaintext   P = P1 P2 P3 ….Pm

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

$$C_1 = P_1 k_{11} + P_2 k_{21} + \cdots + P_m k_{m1}$$
$$C_2 = P_1 k_{12} + P_2 k_{22} + \cdots + P_m k_{m2}$$
$$\cdots$$
$$C_m = P_1 k_{1m} + P_2 k_{2m} + \cdots + P_m k_{mm}$$

C = P. K

The key matrix in the Hill cipher needs to have a multiplicative inverse.

Example

- **Plaintext: "ACT".**
- **Key:** $\begin{pmatrix} A & C & T \end{pmatrix} \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

$$= \begin{pmatrix} 0 & 2 & 19 \end{pmatrix} \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Continue…

$$= \begin{bmatrix} 5 & 21 & 2 \end{bmatrix}$$

Continue...

- $P = C K^{-1}$

for K^{-1},

Step-1 find the det(k)

Step-2 Find the adj(k)

$K^{-1} = \det(k)^{-1} * \text{adj}(k)$

here $\det(k)^{-1}$ is multiplicative inverse of det(k)

Example:

- Plaintext= retreat now
- Key=“backup”

- Ciphertext=SYICHOLER
- Key=“alphabet”

Permutation Cipher/ Transposition Cipher

Permutation Cipher/Transposition Cipher

- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.

Keyless Transposition Cipher

Keyless Transposition Cipher

- Simple transposition ciphers, which were used in the past, are keyless.
- A good example of a keyless cipher using the first method is the **rail fence cipher.**
- Plain Text message "**Meet me at the park**"

m ↘ e ↗ e ↘ t ↗ m ↘ e ↗ a ↘ t ↗ t ↘ h ↗ e ↘ p ↗ a ↘ r ↗ k

m		e		m		a		t		e		a		k
	e		t		e		t		h		p		r	

She then creates the ciphertext "MEMATEAKETETHPR".

Columnar cipher

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

ciphertext “MMTAEEHREAEKTTP”.

Keyed Transposition Cipher

Keyed Transposition Cipher

- The keyless ciphers permute the characters by using writing plaintext in one way and reading it in another way The permutation is done on the whole plaintext to create the whole ciphertext.
- Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

Permutation Cipher

- Alice needs to send the message "Enemy attacks tonight" to Bob..

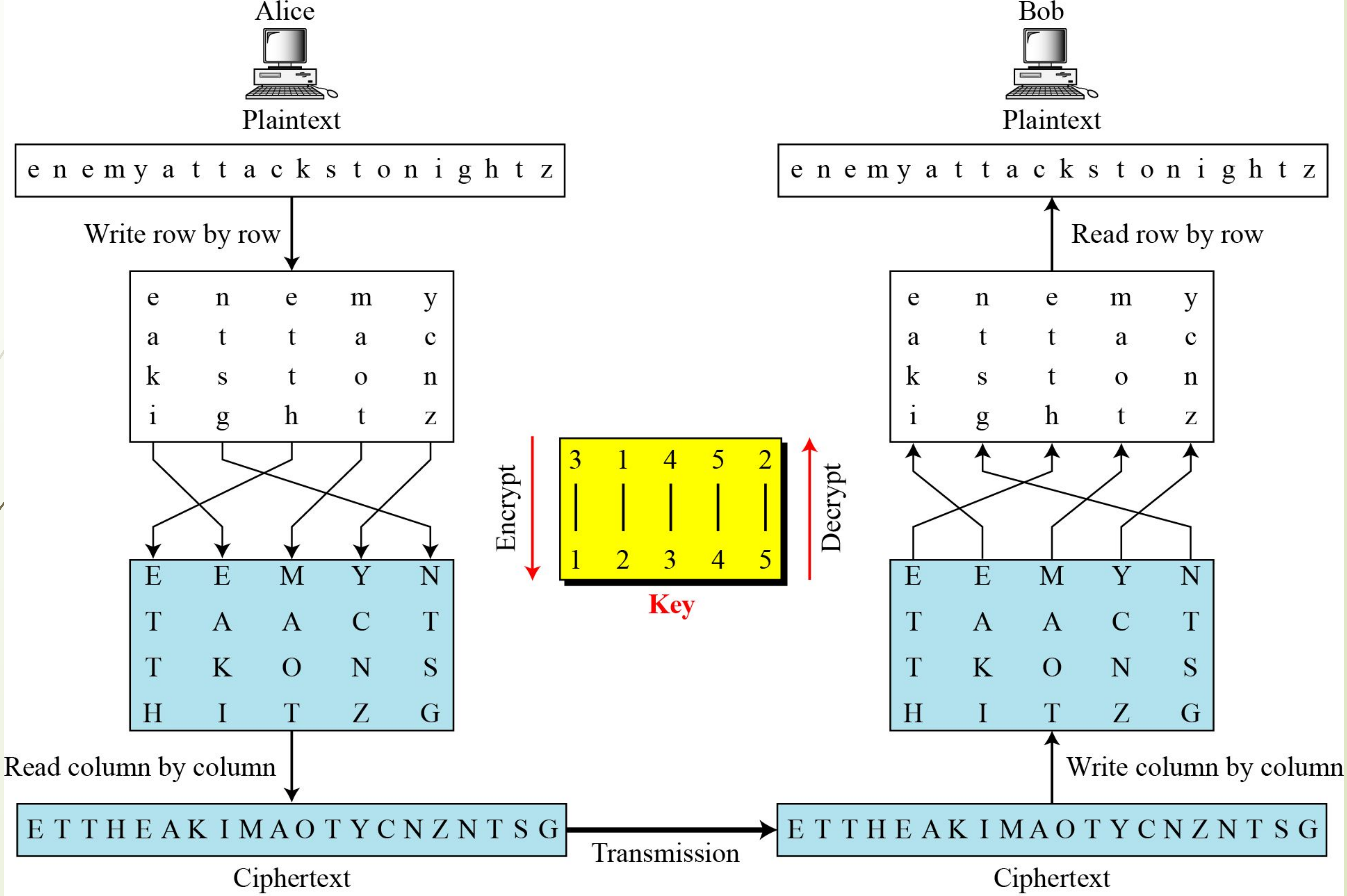
e n e m y a t t a c k s t o n i g h t z

- The key used for encryption and decryption is a permutation key, which shows how the character are permuted.

Encryption ↓	3	1	4	5	2	↑ Decryption
	1	2	3	4	5	

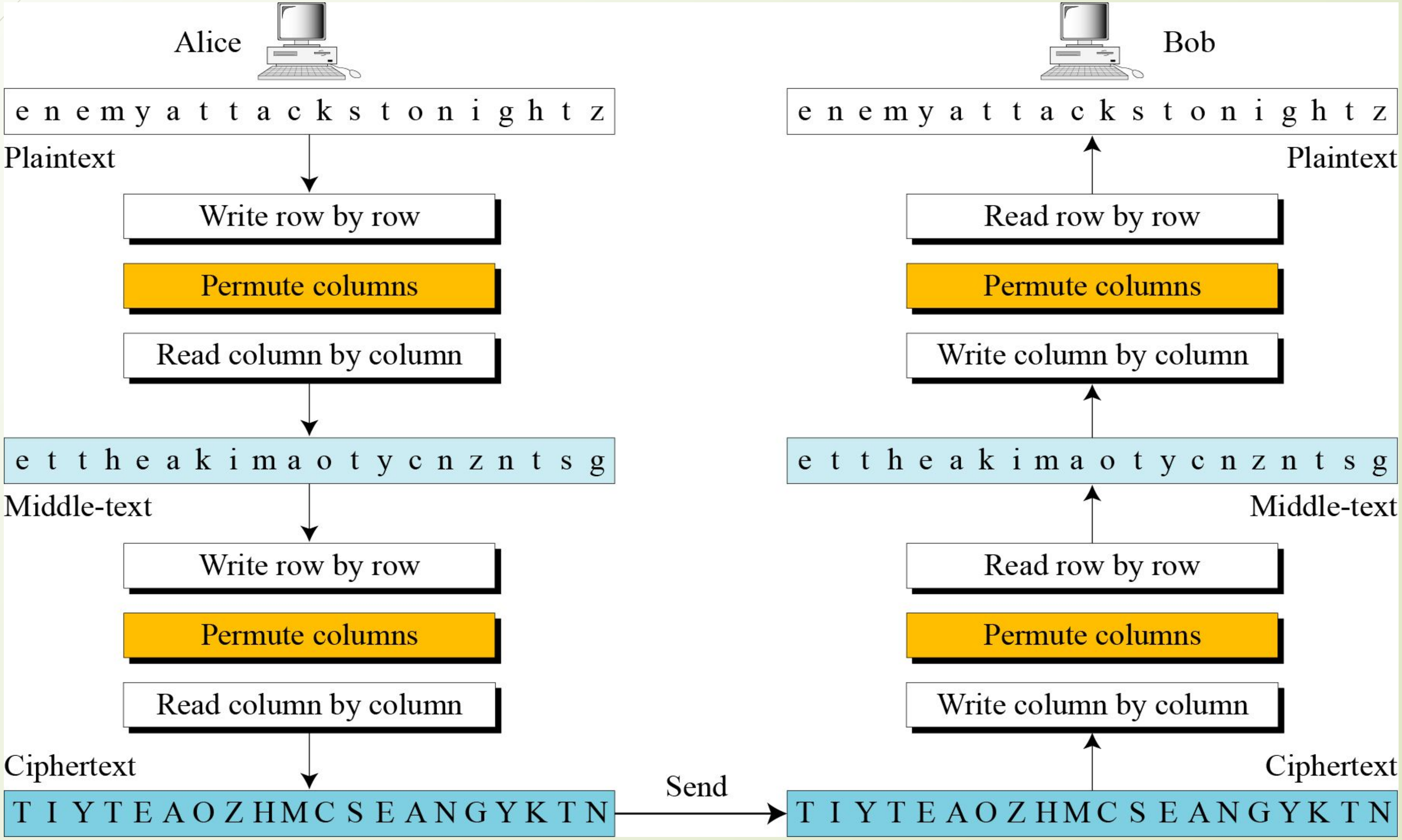
The permutation yields

E E M Y N T A A C T T K O N S H I T Z G



Alice
Plaintext
e n e m y a t t a c k s t o n i g h t z
Write row by row
e n e m y
a t t a c
k s t o n
i g h t z
E E M Y N
T A A C T
T K O N S
H I T Z G
Read column by column
E T T H E A K I M A O T Y C N Z N T S G
Ciphertext
Encrypt
3 1 4 5 2
1 2 3 4 5
Key
Decrypt
Transmission
Bob
Plaintext
e n e m y a t t a c k s t o n i g h t z
Read row by row
e n e m y
a t t a c
k s t o n
i g h t z
E E M Y N
T A A C T
T K O N S
H I T Z G
Write column by column
E T T H E A K I M A O T Y C N Z N T S G
Ciphertext

Double Transposition Cipher



Stream Cipher
vs.
Block Cipher

Stream Cipher

- The literature divides the symmetric ciphers into two broad categories: stream ciphers and block ciphers.
- Call the plaintext stream P, the ciphertext stream C, and the key stream K.

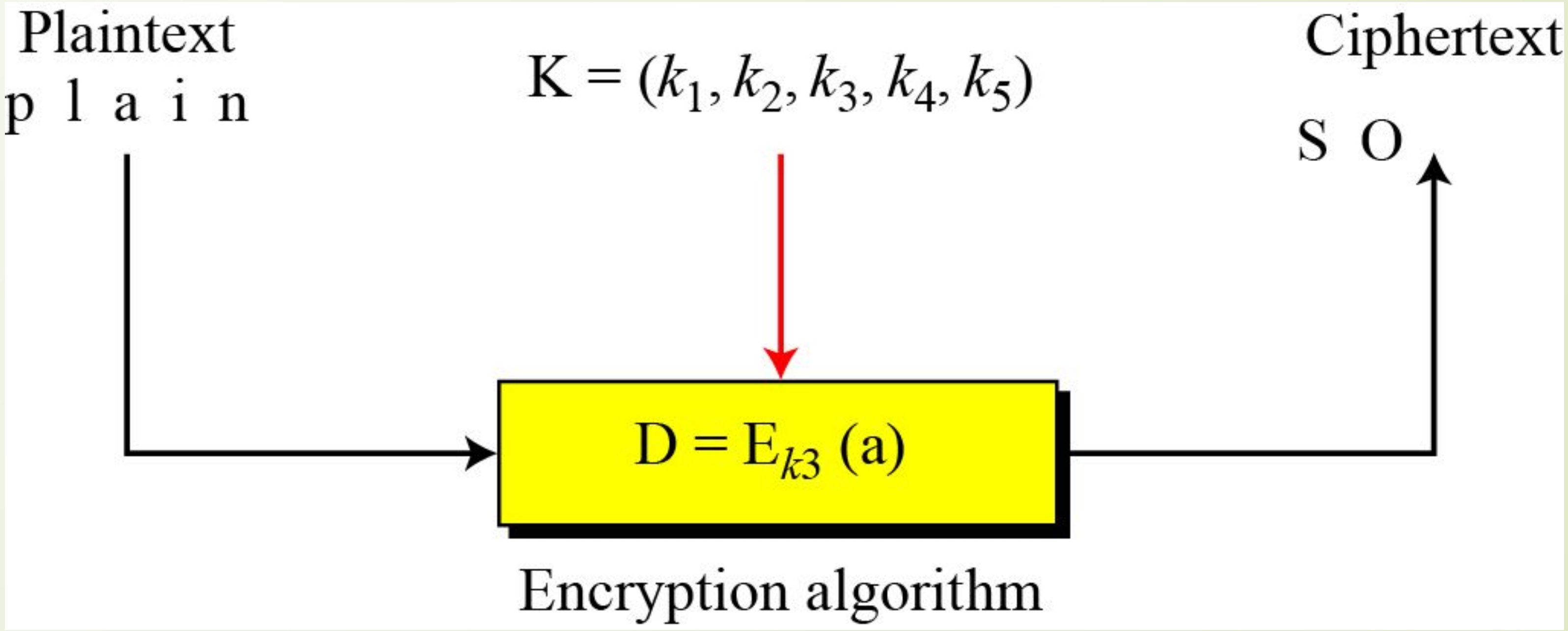
$$P = P_1P_2P_3, \ldots \qquad C = C_1C_2C_3, \ldots \qquad K = (k_1, k_2, k_3, \ldots)$$

$$C_1 = E_{k1}(P_1) \qquad C_2 = E_{k2}(P_2) \qquad C_3 = E_{k3}(P_3) \ \ldots$$

Continue…

Example:

Additive Cipher, Vigenere Cipher, Monoalphabetic Cipher

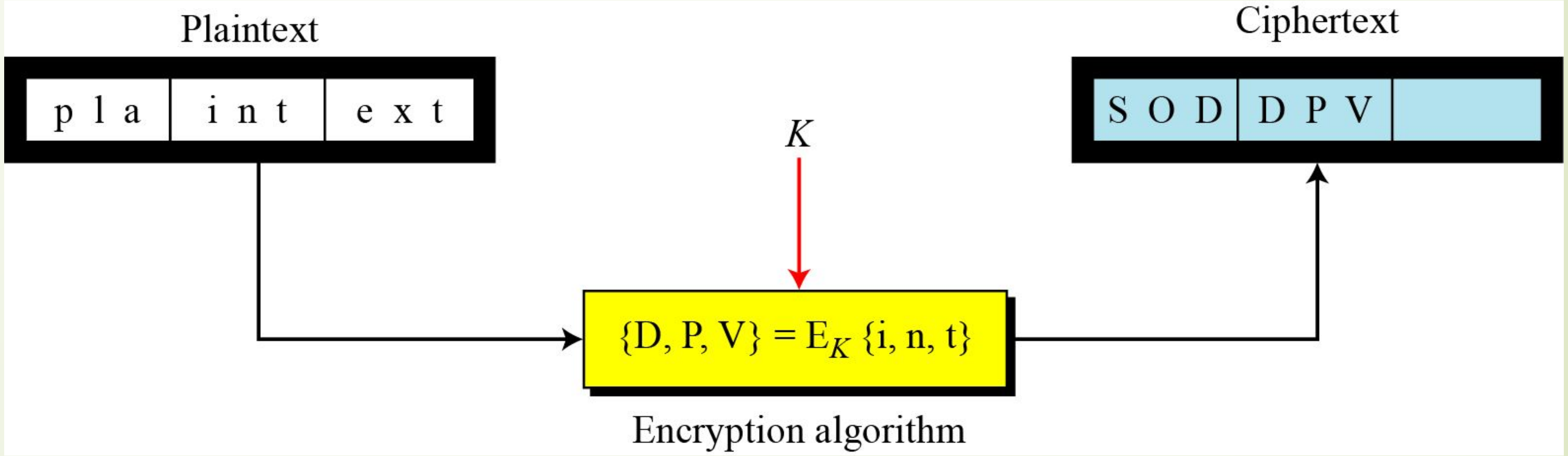


Block Ciphers

- In a block cipher, a group of plaintext symbols of size m ($m > 1$) are encrypted together creating a group of ciphertext of the same size.
- A single key is used to encrypt the whole block even if the key is made of multiple values. Below figure shows the concept of a block cipher.

Continue...

- **Example:** Playfair Cipher, Hill Cipher



Any Questions??

Thank You

References

- Cryptography and network security – Behrouz a forouzan, debdeep mukhopadhyay

Congruence

- Suppose **a and b are integers**, and **m is a positive** integer.
- Then we write **$a \equiv b \pmod{m}$ if m divides $b-a$**.
- The phrase **$a \equiv b \pmod{m}$** is called a congruence, and it is read as "**a is congruent to b modulo m.**" The integer m is called the modulus.

Continue…

- Suppose **we divide a and b by m**, obtaining integer quotients and remainders, where the **remainders are between 0 and m−1.**
- That is, **$a = q_1m + r_1$ and $b = q_2m + r_2$**, where $0 \le r_1 \le m-1$ and $0 \le r_2 \le m-1$.
- Then it is not difficult to see that **$a \equiv b \pmod m$ if and only if $r_1 = r_2$.**
- Thus **$a \equiv b \pmod m$**

  if and only if **$a \bmod m = b \bmod m$**.

Example

$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$

$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

2 Mod 10 will be **2**
12 mod 10 will be **2**

here 2 mod 10= 12 mod 10

So we can write that **2 ≡ 12 (mod 10)**